



**DET KONGELIGE
HELSE- OG OMSORGSDEPARTEMENT**

Statsråden

Kontroll- og konstitusjonskomitéen
Stortinget
0026 OSLO

Deres ref

Vår ref
vk/17/2133

Dato
15. mai 2017

Forespørsel fra kontroll- og konstitusjonskomiteen om nærmere opplysninger om sak om IKT-infrastruktur i Helse Sør-Øst

Jeg viser til brev av 9. mai i år fra Stortingets kontroll- og konstitusjonskomité om ovennevnte.

Jeg har som jeg orienterte om i Stortingets spontanspørretime den 3. mai i år, bedt Helse Sør-Øst RHF om en redegjørelse om saken. Denne vil jeg få 24. mai i år. Helse Sør-Øst RHF har på eget initiativ bedt om en ekstern gjennomgang, gjennomført av PwC. Denne gjennomgangen vil komme i to etapper, med en første leveranse som vil danne grunnlaget for redegjørelsen fra Helse Sør-Øst RHF til meg 24. mai. Gjennomgangen vil bli slutført i løpet av juni.

Redegjørelsen 24. mai vil kunne bidra til å klargjøre flere av de spørsmålene som kontroll- og konstitusjonskomitéen reiser i sitt brev til meg. Jeg vil gjerne få komme tilbake med et nytt brev til komitéen etter at jeg har mottatt redegjørelsen, for slik å kunne gi mest mulig helhetlige og utfyllende svar på de viktige spørsmålene som reises. Svarene jeg gir i brevet må leses i lys av dette.

Min styringsmessige befatning med saken om outsourcing av IKT-infrastrukturen i Helse Sør-Øst skjedde i foretaksrådet 15. september 2016, Sak 3 *IKT-infrastrukturmodernisering i Helse Sør-Øst – godkjenning av finansiell leasing jf. vedtektene §12 Låneopptak*. Følgende beslutning fremgikk i protokollen fra dette foretaksrådet:

"Styret i Helse Sør-Øst RHF behandlet i sak 069-2016 IKT-infrastrukturmodernisering i Helse Sør-Øst. Styret besluttet ved behandling av saken en modernisering av foretaksgruppens IKT-infrastruktur og at dette

gjennomføres ved ekstern leverandør. Da deler av denne tjenesteavtalen kan bli kategorisert som finansiell leasing, ble saken oversendt til behandling i foretaksmøte.

Helse Sør-Øst RHF gjennomgikk saken.

Foretaksmøtet understrekte at avtalen om modernisering av foretaksgruppens IKT-infrastruktur ligger innenfor styrets ansvar for å sørge for en tilfredsstillende organisering av foretakets samlede virksomhet, jf. Lov om helseforetak § 28. Det tilligger derfor styret i Helse Sør-Øst RHF å fatte vedtak om at moderniseringen skal gjennomføres ved ekstern leverandør.

Foretaksmøtet viste til vedtektene § 12, sist endret 7. januar 2015, hvor det bl.a. heter:

"Helse Sør-Øst RHF gis anledning til å inngå finansielle leieavtaler med en kontraktsverdi på inntil 100 mill. kroner pr. avtale. Finansielle leieavtaler utover dette beløpet må forelegges foretaksmøtet."

Foretaksmøtet tok til etterretning at deler av tjenesteavtalen kan bli kategorisert som finansiell leasing og at beløpet kan overstige 100 mill. kroner.

Foretaksmøtet vedtok:

Foretaksmøtet godkjenner, ut fra sak 069-2016 med tilhørende vedtak i styret i Helse Sør-Øst RHF, at deler av tjenesteavtalen som omtales i saken kan innebære finansiell leasing og at beløpet kan overstige 100 mill. kroner".

I foretaksmøtet slo jeg altså fast at arbeidet med modernisering av foretaksgruppens IKT-infrastruktur ligger innenfor styrets ansvar for å sørge for en tilfredsstillende organisering av foretakets samlede virksomhet, jf. lov om helseforetak § 28. Videre at det tilligger styret i Helse Sør-Øst RHF å fatte vedtak om at moderniseringen skal gjennomføres ved bruk av ekstern leverandør. Helse Sør-Øst RHF og helseforetakene har det samlede ansvaret for informasjonssikkerhet og håndtering av personsensitive data i regionen. Min beslutning i foretaksmøtet knyttet seg utelukkende til adgangen til å benytte finansiell leasing for deler av tjenesteavtalen.

Jeg har mottatt flere spørsmål til skriftlig besvarelse fra Stortinget knyttet til outsourcingen av IKT-infrastrukturen i Helse Sør-Øst. Disse spørsmålene har med litt ulike perspektiver tatt opp problemstillinger knyttet til en situasjon hvor deler av driftingen av IKT-infrastrukturen i Helse Sør-Øst overføres til ekstern leverandør, altså en fremtidig situasjon. Dette gjelder spørsmål nr. 1514 (2016) fra representanten Kjersti Toppe, spørsmål nr. 1590 (2016) fra representanten Rasmus Hansson, spørsmål nr. 1627 (2016) fra representanten Olaug V. Bollestad, spørsmål nr. 153 (2016) fra representanten Torgeir Micaelsen, og spørsmål nr. 969 (2017) fra representanten Sverre Myrli, samt spørsmål i interpellasjonsdebatten 10.

november 2016 fra representanten Torgeir Micaelsen. Alle disse svarene baserte seg på informasjon fra Helse Sør-Øst RHF om hvordan IKT-infrastrukturen ville bli håndtert etter at driften i fremtiden blir overført til ekstern leverandør. For å belyse saken på en god måte, er det viktig å skille mellom dagens situasjon der overføring er under planlegging og situasjonen etter at HPE har overtatt driftsansvaret. Denne overføringen har ikke skjedd, og tidspunktet for virksomhetsoverføringen er utsatt. Mine svar til Stortinget er som nevnt basert på hvilket regime som skulle være etablert ved overføring av driften. PwCs endelige rapport vil belyse om de forholdene er godt nok ivaretatt.

Komiteen ber om svar på følgende:

Spørsmål 1. Kan statsråden redegjøre for denne saken og samtidig redegjøre for når departementet har blitt informert om ulike deler av sakskomplekset underveis?

Svar:

Jeg oppfatter at kontroll- og konstitusjonskomiteen er opptatt av tilganger for eksterne IKT-ansatte i forbindelse med planleggingen av overføring av ansvaret for driften av IKT-infrastrukturen, og hvorvidt disse tilgangene har gitt innsyn i personsensitive data. Dette er de samme forholdene som også media har vært opptatt av. Jeg opplever at jeg ikke har fått fullstendig informasjon om dette fra Helse Sør-Øst RHF, og har derfor som nevnt ovenfor, bedt Helse Sør-Øst RHF om en redegjørelse.

Den første faktakunnskap som har blitt gitt departementet knyttet til tilganger i planleggingen av overføringen av driftsansvaret til HPE kom fra Helse Sør-Øst RHF i forbindelse med departementets slutføring av svar på spørsmål til skriftlig besvarelse nr 969 (2017) fra representanten Sverre Myrli. Dette var den informasjonen som ble gitt departementet den 27. april i år, og som nå er alminnelig kjent: "*De ansatte i HPE som i dag har fått tilgang til vår IKT-infrastruktur har fått denne gjennom den såkalte leverandørportalen på lik linje med andre leverandører. Leverandørportalen har egne sikkerhetsmekanismer*". Departementet oppfattet ikke at HPE-ansatte med dette hadde fått tilgang til personsensitive data. Vi oppfattet da at tilgangen gjennom leverandørportalen beskyttet personsensitive data gjennom de nevnte sikkerhetsmekanismene i leverandørportalen. Disse sikkerhetsmekanismene ble også beskrevet i svaret til representanten Myrli. Jeg vil igjen minne om at svaret som ble sendt til representanten Myrli var knyttet til den planlagte situasjonen etter at HPE har overtatt driftsansvar. Jeg hadde derfor på det tidspunktet ikke kunnskap om at det hadde blitt gitt eksterne tilganger som kunne gi mulighet til å tilegne seg personsensitive data under planleggingen av overføringen.

Representanten Micaelsen har i sitt spørsmål til skriftlig besvarelse nr. 1064 (2017) i tillegg spurt om hvilken informasjon jeg hadde fått da jeg møtte i Stortingets spontanspørretime 3. mai i år. Departementet mottok 2. mai en orientering fra administrerende direktør i Helse Sør-Øst RHF. Vi hadde tidligere samme dag fått en intervjuforespørsel fra NRK som beskrev tilgang til personsensitive data. I informasjonen fra Helse Sør-Øst RHF 2. mai gikk det frem at det var gitt midlertidige tilganger for en begrenset periode for 12 ansatte i HPE for

opplæring. Disse tilgangene ble gitt via leverandørportalen og begrenset seg til en definert periode. Disse tilgangene ble ifølge informasjon fra Helse Sør-Øst RHF lukket 27. april da opplæring var gjennomført. Det ble også informert om at det var 16 personer fra HPE som hadde hatt midlertidig tilgang til infrastrukturen for kartlegging. Disse tilgangene ble ifølge Helse Sør-Øst RHF kun benyttet i Sykehuspartners lokaler og under kontroll av Sykehuspartner HF. Disse tilgangene var ifølge Helse Sør-Øst RHF også blitt lukket. Disse opplysningene ga jeg i mitt svar på spørsmål fra representanten Kjersti Toppe i den nevnte spontanspørretimen den 3. mai i år. Da var også saken til NRK publisert. Der mener NRK å kunne dokumentere tilgang av et helt annet omfang. Jeg kunne derfor ikke lenger være trygg på at den informasjonen jeg hadde fått fra Helse Sør-Øst RHF var korrekt. Derfor gjorde jeg det allerede i spontanspørretimen klart at jeg ville be Helse Sør-Øst RHF om en redegjørelse for saken, blant annet fordi jeg opplevde at det var et sprik mellom orienteringer fra Helse Sør-Øst RHF og medias fremstilling av saken. Denne redegjørelsen vil som nevnt ovenfor kunne bidra til å klargjøre flere av de spørsmålene som kontroll- og konstitusjonskomiteen reiser i sitt brev til meg, og jeg vil derfor komme tilbake til komiteen med et mer helhetlig og utfyllende svar.

Spørsmål 2. Kan statsråden nå gi en oversikt over hvem som har hatt tilgang på informasjon de ikke skulle ha hatt tilgang på?

Svar:

Det vises til omtale over av den gjennomgangen som skal gjennomføres av PwC. Del I av dette oppdraget vil som nevnt utgjøre den redegjørelsen jeg har bedt om å få fra Helse Sør-Øst RHF, og som jeg vil motta 24. mai. I engasjementsbrevet (vedlagt) heter det blant annet:

"Del I av oppdraget skal blant annet belyse følgende forhold:

- En oppdatert status på gjennomføringen av programmet i Sykehuspartner
- Programmets kontrollregime knyttet til oppfyllelse av krav til informasjonssikkerhet, spesifikt:
 - Fakta om tilganger som er gitt, om de er gitt etter gjeldende rutiner, om det anses forsvarlig at disse tilgangene er gitt og om rutinene er forsvarlige
 - Undersøke eventuelt misbruk av tilganger og om personsensitive data har kommet på avveie
- Vurdering av systemet for gjennomføring av risikovurderinger i programmet knyttet til informasjonssikkerhet
- Om Helse Sør-Øst RHF har fått tilstrekkelig informasjon om risiko og gjennomføringen av programmet vedrørende informasjonssikkerhet
- Andre relevante forhold

Basert på gjennomgangen skal det identifiseres tiltak som sikrer gjennomføring av programmet og/eller bidrar til å redusere risiko."

Av dette går det frem at jeg etter at denne redegjørelsen er gjennomført vil ha et langt bedre grunnlag for å gi et presist svar på spørsmålet. Jeg ber derfor om å få komme tilbake til dette etter at redegjørelsen foreligger.

Spørsmål 3. Har statsråden grunn til å tro at informasjon om norske pasienter kan ha kommet på avveie?

Svar:

Jeg har ikke mottatt informasjon om at pasientopplysninger har kommet på avveie. Dette er et svært sentralt spørsmål som vil bli belyst i redegjørelsen fra Helse Sør-Øst RHF, jf. at PwC er bedt om å undersøke eventuelt misbruk av tilganger og om personsensitive data har kommet på avveie. Dette er også et spørsmål jeg vil komme tilbake til etter at redegjørelsen foreligger.

Spørsmål 4. Hva er departementets vurdering av skadeomfanget dersom pasientopplysninger har kommet på avveie, og hva er departementets vurdering av alvoret i denne saken?

Svar:

Jeg har som nevnt ikke mottatt informasjon om at pasientopplysninger har kommet på avveie. Hvis redegjørelsen fra Helse Sør-Øst RHF viser at det har kommet pasientopplysninger på avveie, så er dette selvfølgelig alvorlig. Det er vanskelig for meg nå å spekulere i et potensielt skadeomfang knyttet til at slike opplysninger skulle vise seg å være på avveie.

Spørsmål 5. Hva har statsråden gjort for å sikre seg om at denne saken ryddes opp i?

Svar:

Jeg har bedt om en redegjørelse fra Helse Sør-Øst RHF. Denne redegjørelsen vil gi grunnlag for en bedre forståelse av fakta i saken, og gjennom det også gi meg et bedre grunnlag for å vurdere om jeg bør gjøre noen styringsmessige grep. Redegjørelsen vil dessuten gi Helse Sør-Øst RHF et bedre grunnlag for å vurdere om det er behov for ytterligere tiltak for å sikre informasjonssikkerheten i regionen.

Jeg vil ellers understreke at Helse Sør-Øst RHF har informert departementet om at de har lukket alle tilganger til IKT-infrastrukturen for ansatte i HPE knyttet til programmet for modernisering av IKT-infrastruktur.

Spørsmål 6. Er det riktig det som statsråden sa i Stortinget i interpellasjonsdebatten 10. november 2016 om at: "...personopplysninger ikke skal overføres til andre land ..."?

Svar:

Interpellasjonsdebatten i Stortinget 10. november 2016 handlet om den fremtidige situasjonen etter at drift av IKT-infrastruktur var overført til en ekstern leverandør. Som tidligere opplyst i brevet har overføringen til HPE ennå ikke skjedd. De tilganger som har blitt gitt, og som ifølge Helse Sør-Øst RHF nå er lukket, har vært knyttet til en planleggings- og opplæringsfase. Mine svar i interpellasjonsdebatten omhandlet det sikkerhetsregimet som skal være på plass etter at driften er overført til ekstern leverandør.

Jeg vil igjen være klar på at jeg forventer at kun personell som har lovlig adgang skal ha tilgang til sensitive data. Dette er noe jeg vil ha spesiell oppmerksomhet på når gjennomgangen fra PwC foreligger (del I og del II).

Jeg vil avslutningsvis igjen presisere at jeg ønsker å få komme tilbake med et nytt brev til Stortingets kontroll- og konstitusjonskomite med et mer helhetlig og utfyllende svar på de viktige spørsmålene som komiteen reiser i sitt brev til meg. Dette vil jeg gjøre innen 1. juni i år, etter at jeg har mottatt redegjørelsen fra Helse Sør-Øst RHF den 24. mai i år.

Med hilsen



Bent Høie

Vedlegg: Engasjementsbrev PwC datert 9. mai 2017